



Affects Members Of the Public?	Mark if Applicable w/ an X
--------------------------------	----------------------------

Department of Energy Privacy Impact Assessment (PIA)

Guidance is provided in the template. See DOE Order 206.1, *Department of Energy Privacy Program, Appendix A, Privacy Impact Assessments*, for requirements and additional guidance for conducting a PIA: https://www.directives.doe.gov/directives-documents/200-series/0206.1-BOrder/@_images/file

Please complete form and return via email to Privacy@hq.doe.gov

No hand-written submissions will be accepted.

This template may not be modified.

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	June 14, 2021	
Departmental Element & Site	U.S. Department of Energy, Office of Energy Efficiency and Renewable Energy (EERE). This system is located at the US Department of Energy Headquarters, 1000 Independence Avenue, EERE Server Room, Washington D.C. 20585	
Name of Information System or IT Project	Federal Energy Management Program (FEMP) Compliance Tracking System (CTS), part of the EERE Centralized Web Hosting Environment (ECWHE)	
Exhibit Project UID	019-000000141 00-20-02-00-02-00	
New PIA Update	<input type="checkbox"/> <input checked="" type="checkbox"/>	CTS PIA is updated as part of the annual review/update. No changes on PII collection/maintenance.
	Name, Title	Contact Information Phone, Email
System Owner	Chris Tremper, Program Analyst Federal Energy Management Program	(202) 586-7632 Chris.Tremper@ee.doe.gov
Local Privacy Act Officer	Shaida Beklik, Cyber Security Program Manager (CSPM)	(202) 586-4769 Shaida.Beklik@ee.doe.gov
Cyber Security Expert reviewing this	Shaida Beklik, CSPM	(202) 586-4769 Shaida.Beklik@ee.doe.gov



MODULE I – PRIVACY NEEDS ASSESSMENT

document (e.g. ISSM, CSSM, ISSO, etc.)		
Person Completing this Document	Chris Tremper	(202) 586-7632 Chris.Tremper@ee.doe.gov
Purpose of Information System or IT Project	<p>The Compliance Tracking System (CTS) is a Web-based data collection and reporting system for Federal facilities mandated by Section 432 of the Energy Independence and Security Act of 2007 (EISA), for the management of energy and water efficiency. CTS serves as a repository for all facility level data required by EISA 432, which includes name, email address, and phone number.</p> <p>CTS data collected relates to facility energy and water use and efficiency at individual facilities. The name or agency identifier (optional) of the related energy managers is also stored. In addition, names, email addresses, and phone numbers (phone numbers are optional to provide) of system users are stored in the system. An agency can list its manager at each of its sites (optional).</p>	
Type of Information Collected or Maintained by the System:	<ul style="list-style-type: none"> <input type="checkbox"/> SSN Social Security number <input type="checkbox"/> Medical & Health Information e.g. blood test results <input type="checkbox"/> Financial Information e.g. credit card number <input type="checkbox"/> Clearance Information e.g. "Q" <input type="checkbox"/> Biometric Information e.g. finger print, retinal scan <input type="checkbox"/> Mother's Maiden Name <input type="checkbox"/> DoB, Place of Birth <input type="checkbox"/> Employment Information <input type="checkbox"/> Criminal History <input checked="" type="checkbox"/> Name <input checked="" type="checkbox"/> Other – Phone, email address, and phone number (optional) 	



MODULE I – PRIVACY NEEDS ASSESSMENT

<p>Has there been any attempt to verify PII does not exist on the system?</p> <p><i>DOE Order 206.1, Department of Energy Privacy Program, defines PII as any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.</i></p>	<p>No, PII is knowingly collected by the application and stored within the system.</p>
<p>If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)</p>	<p>N/A</p>

Threshold Questions

<p>1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?</p>	<p>YES</p>
<p>2. Is the information in identifiable form?</p>	<p>YES</p>
<p>3. Is the information about individual Members of the Public?</p>	<p>NO</p>
<p>4. Is the information about DOE or contractor employees?</p>	<p>YES</p> <p><input checked="" type="checkbox"/> Federal Employees</p> <p><input checked="" type="checkbox"/> Contractor Employees</p>

If the answer to **all** four (4) Threshold Questions is "No," you may **proceed to the signature page of the PIA**. Submit the completed PNA with signature page to the CPO.

Module II must be completed for all systems if the answer to any of the four (4) threshold questions is "Yes." All questions must be completed. If appropriate, an answer of N/A may be entered.

The goal of the threshold questions is to legitimately and efficiently determine whether additional assessment is necessary. If there is doubt, it is in the System Owner's best interest to complete Module II.



MODULE I – PRIVACY NEEDS ASSESSMENT

PIAs affecting Members of the Public are posted on the DOE Privacy website. For this reason, PIAs affecting Members of the Public should be written in plain language and at a high level so they are easily understandable and do not disclose sensitive information.

END OF PRIVACY NEEDS ASSESSMENT

MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE

<p>1. AUTHORITY</p> <p>What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?</p>	<p>42 U.S.C. § 8253 (f)(7)(B)</p>
<p>2. CONSENT</p> <p>What opportunities do individuals have to decline to provide information (e.g. where providing information is voluntary) or to consent only to particular uses of the information (other than required or authorized uses)?</p>	<p>A valid email address is required to log into the system. The first and last names of the system users are saved with the user account. Work phone number is optional to provide. An individual does have the opportunity to decline to provide PII, but he/she will not be able to log into the system to participate in the program.</p>
<p>3. CONTRACTS</p> <p>Are contractors involved with the design, development and maintenance of the system? If yes, was the Privacy Order CRD or Privacy Act clauses included in their contracts?</p>	<p>Yes, contractors are involved with the design, development, and maintenance of the system. Privacy Act clauses are included in their contracts.</p>



MODULE II – PII SYSTEMS & PROJECTS

<p>4. IMPACT ANALYSIS: How does this project or information system impact privacy?</p>	<p>Names, email addresses, and phone numbers (phone numbers are optional to provide) maintained in CTS are low risk and non-sensitive PII. The data is only available to system administrators or individuals designated by the system owner who have oversight responsibility of agency information.</p> <p>CTS is designed to protect PII and mitigate privacy risk via the following administrative, technical, and physical controls:</p> <ul style="list-style-type: none"> • Strict access control enforcement based on need-to-know • Password • Security scans <p>The potential for privacy concerns if the system happened to be compromised is low, as the information is not personal and generally available to the public.</p>
<p>5. SORNs How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)? If yes, explain, and list the identifiers that will be used to retrieve information on the individual.</p>	<p>The username list that contains names and email addresses may be sorted or filtered by the email address or first or last name. However, PII data is not retrieved by the system via unique identifier. Access to the username list is limited to the system administrator or individuals designated by the system owner who have oversight responsibility of this data.</p>
<p>6. SORNs Has a Privacy Act System of Records Notice (SORN) been published in the <i>Federal Register</i>? If "Yes," provide name of SORN and location in the <i>Federal Register</i>.</p>	<p>N/A. CTS does not maintain data on individuals nor retrieve PII via unique identifier, see #5 above. The system's data collected relates to facility energy and water use and efficiency at Federal facilities.</p>
<p>7. SORNs If the information system is being modified, will the SORN(s) require amendment or revision?</p>	<p>N/A</p>



MODULE II – PII SYSTEMS & PROJECTS

DATA SOURCES

<p>8. What are the sources of information about individuals in the information system or project?</p>	<p>The information is provided either directly by the individual (system user) or organizational administrator.</p>
<p>9. Will the information system derive new or meta data about an individual from the information collected?</p>	<p>No</p>
<p>10. Are the data elements described in detail and documented?</p>	<p>Yes – data elements are described in a data dictionary and database schema.</p>

DATA USE

<p>11. How will the PII be used?</p>	<p>Email addresses are used for system login and to provide a user agency POC for the information submitted to the system.</p> <p>Names and email addresses are also used to associate the energy manager with a facility record, and to monitor user account requests and data changes.</p>
<p>12. If the system derives meta data, how will the new or meta data be used?</p> <p>Will the new or meta data be part of an individual's record?</p>	<p>N/A – The system does not derive meta data.</p>
<p>13. With what other agencies or entities will an individual's information be shared?</p>	<p>The individual's information within the system will not be shared with any other agencies or entities.</p>

Reports



MODULE II – PII SYSTEMS & PROJECTS

<p>14. What kinds of reports are produced about individuals or contain an individual's data?</p>	<p>Internal reports show what facility an individual is associated with and if that person is an energy manager at that facility. The internal reports provide information including the energy manager's name, ID, and email address, and what agency the individual is reporting from.</p> <p>System reports are available to agency administrators which identify system activity (data changes, including names of those who modified their information) associated with a user account. The data changes are available to program administrators.</p>
<p>15. What will be the use of these reports?</p>	<p>Agency internal use; to assess compliance with the requirement for assigned energy managers at covered facilities.</p>
<p>16. Who will have access to these reports?</p>	<p>System Administrators and individuals designated by the System Owner who have oversight responsibility of this data will have access to these reports. Individuals who voluntarily provide their PII will not have access to these reports – it depends on the level of each individual, according to level of access and permissions of each individual.</p>
<p>Monitoring</p>	
<p>17. Will this information system provide the capability to identify, locate, and monitor individuals?</p>	<p>The system does not identify, locate, and/or monitor individuals.</p>
<p>18. What kinds of information are collected as a function of the monitoring of individuals?</p>	<p>N/A – The system does not collect information as a function of monitoring individuals.</p>
<p>19. Are controls implemented to prevent unauthorized monitoring of individuals?</p>	<p>Yes. Although the application does not have monitoring capabilities, EERE and CTS have implemented security controls to prevent unauthorized users from monitoring or accessing any of the PII on the system (e.g., Access Controls).</p>
<p>DATA MANAGEMENT & MAINTENANCE</p>	
<p>20. How will records about individuals be kept current and verified for accuracy, relevance and completeness? Include PII data collected from sources other than DOE records.</p>	<p>Users or administrators are responsible for updating the email address and phone number (phone numbers are optional to provide by the individual) if they change. System administrators hold bi-monthly meeting workgroups to encourage system users to update their information. There are no individual/automatic checks to determine whether PII is accurate and complete.</p>



MODULE II – PII SYSTEMS & PROJECTS

<p>21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?</p>	<p>N/A – The system is only operated at one site which is in the EERE Server Room at DOE’s Headquarters location.</p>
<p>Records Management</p>	
<p>22. Identify the record(s).</p>	<ul style="list-style-type: none"> • Covered Facility Characteristics • Covered Facility Energy Use and Energy Manager Assignment • Covered Facility Annual Footprint • Covered Facility Year by Year Trends (by Agency) • Comprehensive Evaluation Compliance • Comprehensive Evaluation Findings • Facility Evaluation Status • Initiated Projects • Project Follow-up Activity, Benchmarked buildings • Measured Project Savings in Energy Goal-Excluded Facilities • Benchmarking Metrics • Benchmarking Year by Year Trends (by Agency).
<p>23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.</p>	<p>Unscheduled</p>
<p>24. Records Contact</p>	<p>Tia Alexander 202-586-3135 Tia.Alexander@ee.doe.gov</p>
<p>ACCESS, SAFEGUARDS & SECURITY</p>	
<p>25. What controls are in place to protect the data from unauthorized access, modification or use?</p>	<p>CTS has physical and logical security controls in place to prevent unauthorized access, modification, and use. The System Owner has implemented NIST 800-53 baseline security controls appropriate to its FIPS categorization, in accordance with DOE Directives and the Office of the Under Secretary of Energy Implementation Plan for the Department’s Risk Management Approach (Energy Programs RMA IP). Access controls (username/password, role based access privileges) are in place to protect the confidentiality and integrity of the CTS data. Regularly scheduled security scans are also performed on CTS. In addition, security assessments are conducted on an annual basis using the NIST SP 800-53 methodology.</p>



MODULE II – PII SYSTEMS & PROJECTS

<p>26. Who will have access to PII data?</p>	<p>System Administrators and individuals designated by the System Owner who have oversight responsibility of this data will have access to PII data. Individuals who input their own PII voluntarily into the system will have access to change their own PII.</p>
<p>27. How is access to PII data determined?</p>	<p>The system implements role-based access controls and PII data is made available only to individuals designated by the System Owner who have oversight responsibility of this data.</p>
<p>28. Do other information systems share data or have access to the data in the system? If yes, explain.</p>	<p>No. The CTS is a stand-alone application and does not share or provide access of data electronically to any other systems.</p> <p>Reports may be exported in Excel; Web Services allow input (not output) of data.</p>
<p>29. For connecting information systems, is there an Interconnection Security Agreement (ISA) or other agreement between System Owners to ensure the privacy of individuals is protected?</p>	<p>N/A – CTS is a stand-alone application and is not connected to any other system. Therefore, an agreement or ISA is not required.</p>
<p>30. Who is responsible for ensuring the authorized use of personal information?</p>	<p>System Owner</p>

END OF MODULE II



SIGNATURE PAGE		
	Signature	Date
System Owner	<p>Christopher L. Tremper</p> <hr/> <p>(Print Name)</p> <p><i>Christopher L. Tremper</i></p> <hr/> <p>(Signature)</p>	<p>6/15/2021</p> <hr/>
Local Privacy Act Officer	<hr/> <p>(Print Name)</p> <hr/> <p>(Signature)</p>	<hr/>
W. Ken Hunt Chief Privacy Officer	<hr/> <p>(Print Name)</p> <hr/> <p>(Signature)</p>	<hr/>